ANNEX
ENGLISH TRANSLATION OF CLAIMS
AS AMENDED IN THE INTERNATIONAL APPLICATION

NATIONAL PHASE SUBMISSION

Patent claims

1. An integrated circuit (1) comprising function modules (2), wherein the function modules (2) comprise a central processing unit (4), by means of which data can be processed and programs can be executed, and a cache memory (5), wherein the function modules (2) comprise an encryption unit (6) by means of which data can be encrypted and decrypted and the function modules (2) comprise a security sensor system (9) by means of which at least one operating parameter (f, T, U) of the integrated circuit (1) can be monitored, characterized in that, as operating parameters (f, T, U), the state of a protective layer (20) on the integrated circuit (1) is monitored.

2. The integrated circuit (1) as claimed in claim 1, characterized in that the function modules comprise a random-number generator (80).

3. The integrated circuit (1) as claimed in claim 1, characterized in that the function modules (2) comprise a first memory (7) in which cryptological keys (18) are stored.

4. The integrated circuit (1) as claimed in claim 2 and 3, characterized in that cryptological keys (18) which are stored in the first memory (7) are generated by means of the random-number generator (80).

5. The integrated circuit (1) as claimed in claim 1, characterized in that function modules (2) comprise a real-time clock (8).

ANNEX
ENGLISH TRANSLATION OF CLAIMS
AS AMENDED IN THE INTERNATIONAL APPLICATION

NATIONAL PHASE SUBMISSION

6. The integrated circuit (1) as claimed in claim 1, characterized in that operating parameters (f, T, U) to be monitored additionally is the clock frequency (f) of the real-time clock (8) and/or an operating temperature (T) at a point in the integrated circuit (1) and/or an operating voltage (U) of the integrated circuit (1).

7. The integrated circuit (1) as claimed in claim 1, characterized in that at least one limit value is predetermined for the operating parameter (f, T, U) to be monitored, the operating parameter (f, T, U) is measured and compared with the limit value and when the result exceeds or drops below the limit value, the content of the first memory is deleted.

8. The integrated circuit (1) as claimed in claim 1, characterized in that it is arranged in a package (30) and has terminal contacts (31) brought out of the package (30).

9. The integrated circuit (1) as claimed in claim 1, characterized in that individual function modules (2) have an essentially planar extent and are arranged adjacently to one another in the area of the normal to the surface.

10. The integrated circuit (1) as claimed in claim 1, characterized in that the function modules (2) comprise an integrated voltage regulator which regulates an operating voltage (U).

11. The integrated circuit (1) as claimed in claim 1, characterized in that it is constructed as semiconductor chip (13).

ANNEX
ENGLISH TRANSLATION OF CLAIMS
AS AMENDED IN THE INTERNATIONAL APPLICATION

NATIONAL PHASE SUBMISSION

12. The integrated circuit (1) as claimed in claim 11, characterized in that semiconductor structures of the individual function modules (2) are intermeshed in the manner of a puzzle in order to avoid individual function modules (2) from being recognizable.

13. The integrated circuit (1) as claimed in claim 11, characterized in that an active protective layer (20) which consists of at least one elongated electrical line (21) which extends along the surface of the die, particularly in mutually parallel tracks section by section, is applied directly to the die of the semiconductor chip (13).

14. An arrangement comprising an integrated circuit (1) as claimed in one of claims 1 to 13, characterized in that the integrated circuit (1) is connected by means of a data bus (32) to a second memory (40) [RAM] in which data are stored encrypted, wherein the second memory (40) has memory cells which in each case have a memory address and each memory cell can be addressed directly in reading or writing manner.

15. The arrangement comprising an integrated circuit (1) as claimed in one of claims 1 to 13, characterized in that the second memory (40) is volatile and is connected to a battery (43) so that the voltage supply is maintained when another power supply is lacking.

16. The arrangement comprising an integrated circuit (1) as claimed in one of claims 1 to 13, characterized in that the integrated circuit (1) is connected by means of a data bus (32)

ANNEX
ENGLISH TRANSLATION OF CLAIMS
AS AMENDED IN THE INTERNATIONAL APPLICATION

NATIONAL PHASE SUBMISSION

to a non-volatile third memory (41), particularly a flash memory or ROM, in which data or program code are stored encrypted.

17. The arrangement comprising an integrated circuit (1) as claimed in claim 1, characterized in that the security sensor system (9) is connected to a battery (43) so that the voltage supply is maintained if another power supply is lacking.

18. The arrangement comprising an integrated circuit (1) as claimed in claim 1, characterized in that the security sensor system (9) is connected to an auxiliary power source (12), integrated in the package (30), which provides the power for deleting the first memory (7).